Les paiements électroniques au regard de la vente à distance

Salaun, Anne

Published in:
I nuovi diritti nell'integrazione europea : la tutela dell'ambiente e la protezione del consumatore. Progetto Jean Monnet, Padova, 11-15 gennaio 1999

Publication date:
2000

Document Version
le PDF de l'éditeur

Les paiements électroniques au regard de la vente à distance

ANNE SALAÜN
Université Namur - Centre de Recherches Informatique et Droit

1. L'émergence du commerce par Internet suscite des perspectives commerciales immenses. Il est désormais possible de faire ses courses sur Internet, de commander des biens et des services, de consulter des sites d'informations, de télécharger des renseignements sur son ordinateur, tout cela sans notion de frontières: les transactions peuvent aussi bien se réaliser avec un opérateur implanté à quelques kilomètres de chez soi qu'à l'autre bout du monde ...

Le développement de ce nouveau type de commerce génère de nouvelles préoccupations pour l'utilisateur au sujet de la sécurité des paiements effectués par voie électronique. Très souvent, le système de paiement requiert la transmission du numéro de la carte de crédit du client et sa date d'échéance. Comment alors être sûr que ce numéro ne sera pas intercepté lors de sa transmission par le biais du réseau et utilisé frauduleusement par un tiers? De plus, comment garantir au client que seul le montant du bien ou du service commandé lui sera débité?

La récente recommandation de la Commission européenne relative aux "opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire"[1], tente de répondre à ces préoccupations. La volonté affichée par la Commission européenne dans ce texte est de parvenir à une confiance totale des utilisateurs, et d'assurer un degré élevé de protection des consommateurs dans l'utilisation des moyens de paiement électroniques[2]. Le développement serein du commerce électronique passe nécessairement par une sécurisation des paiements qui s'y effectuent. Au demeurant, cette idée est confortée par la volonté européenne de faire du

[1] Recommandation en date du 30 juillet 1997, *J.O.C.E.* L 208 du 2 août 1997.
[2] Considérant 8 de la recommandation.

commerce électronique "grand public" une priorité[3]. Le développement des systèmes de paiement ne peut se faire que dans le respect des intérêts de toutes les parties au système: les institutions émettrices, les commerçants et les consommateurs.

Le présent article se propose d'établir le lien entre la recommandation et la vente à distance qui se réalise par voie électronique[4]. Les contrats conclus par voie électronique sont en effet régis par la nouvelle législation européenne relative aux contrats à distance[5], qui oblige les États membres à prendre les mesures appropriées pour que le consommateur puisse demander l'annulation d'un paiement en cas d'utilisation frauduleuse de sa carte, et soit recrédité des sommes versées en paiement[6].

Après une analyse de la recommandation de 1997 et de son intérêt par rapport aux deux recommandations précédentes (I), l'article se concentrera sur les spécificités des contrats à distance et examinera dans quelle mesure la recommandation peut répondre aux attentes de protection des consommateurs en matière de paiement électronique (II).

I. La recommandation du 30 juillet 1997

2. La recommandation est précédée d'une communication intitulée "accroître la confiance des utilisateurs dans les moyens électroniques de paiement dans le cadre du marché unique"[7]. Les quatre objectifs de cette communication sont 1) de définir un cadre de surveillance approprié, 2) de fournir des lignes directrices en matière de transparence, de responsabilité et de voies de recours, 3) d'éclairer les conditions d'application des règles communautaires de concurrence pour parvenir à un équilibre approprié entre besoin d'interopérabilité

[3] Idée énoncée dans une communication de la Commission européenne au Parlement européen, au Conseil au Comité Économique et Social et au Comité des Régions en date du 12 avril 1997: "A European initiative in electronic commerce" (texte disponible à l'adresse suivante: http://www.ispo.cec.be/Ecommerce).

[4] Cet article s'inscrit dans le cadre d'un contrat de recherches entre le CRID et le Ministère belge des Affaires Économiques.

[5] Directive 97/7/CE du Parlement Européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, *J.O.C.E.* L 144 du 4 juin 1997. La directive doit être transposée par les États membres au plus tard 3 ans après son entrée en vigueur, soit le 4 juin 2000.

Pour une analyse des caractéristiques d'une transaction commerciale sur Internet, v. Y. BRULARD et P. DEMOLIN, *Internet face au droit*, in Les Cahiers du CRID n° 12, 11.

[6] Directive contrats à distance, art. 8 "paiement par carte".

[7] COM (97) 353 final.

et nécessité d'une concurrence saine et vigoureuse, et 4) de prévenir les risques d'utilisation frauduleuse et de contrefaçons en améliorant la sécurité.

L'on pourrait s'interroger sur l'opportunité du choix d'une recommandation, instrument juridique non contraignant – au même titre que l'avis – selon l'art. 189 du Traité de Rome, qui ne lie pas les États membres destinataires. Le Comité Consultatif de la Consommation s'était d'ailleurs, en son temps, ému de ce choix en arguant de la stratégie affichée de la Commission qui, dans un document intitulé "*Europe could play an ace*" de 1987, avait prévu d'adopter une directive en cette matière[8]. Toutefois, le caractère facultatif de la recommandation ne doit pas préjuger de sa "force" politique qui doit amener les États membres – et les organismes concernés – à un examen minutieux du texte. La précédente recommandation de 1988 en est l'illustration parfaite: les trois fédérations européennes du secteur du crédit avaient présenté en 1989, en réponse à la recommandation relative aux systèmes de paiement du 17 novembre 1988[9], un "*Code of Best Practice*"[10]. Ces fédérations, qui avaient critiqué certaines dispositions de la recommandation, avaient néanmoins pris en compte les exigences de la Commission en matière de protection des consommateurs. Un texte remanié, renommé "*Code de bonne conduite*", avait été présenté à la Commission européenne, en novembre 1990, comme réponse définitive des banques à la recommandation de 1988.

Les parties concernées par la recommandation doivent se conformer avec ses dispositions, mais sont libres quant au choix des moyens techniques à mettre en œuvre pour assurer la sécurité des paiements électroniques. La Commission a en effet choisi de ne pas imposer de cadre strict pour la mise en œuvre des principes, pourvu que ceux-ci soient retenus. Elle entend en effet suivre la mise en œuvre de la recommandation. Elle donne à cet effet comme date butoir le 31 décembre 1998 pour que les États membres prennent les mesures nécessaires afin que les émetteurs d'instruments de paiement électronique se mettent en conformité avec la recommandation[11]. Ce n'est que

[8] Document COM (86) 754 final, 12 janvier 1987. V. également l'art. de C. KNOBBOUT-BETHLEM sur la recommandation de 1987, in *REDC* 1990, 243.

[9] V. *infra* point 5.

[10] Les trois fédérations sont la Fédération bancaire de la Communauté Européenne, le Groupement des Banques Coopératives de la Communauté Européenne et le Groupement Européen des Caisses d'Épargne, toutes regroupées dans l'AESC (Associations européennes du secteur du crédit). V. pour plus de renseignements l'ouvrage de X. FAVRE-BULLE, *Le droit communautaire du paiement électronique*, Zurich, 1992, 66.

[11] Art. 11 de la Recommandation.

dans le cas où elle jugerait les résultats insatisfaisants qu'elle proposera une législation contraignante[12].

A. Historique

3. La recommandation de 1997 fait suite à deux initiatives communautaires lancées depuis 1987: une première recommandation avait en effet été adoptée le 8 décembre 1987 au sujet d'un code européen de bonne conduite en matière de paiement électronique[13], aussitôt suivie par une seconde recommandation concernant les systèmes de paiement et en particulier les relations entre titulaires et émetteurs de cartes, adoptée le 17 novembre 1988[14].

1. La recommandation du 8 décembre 1987

4. La raison d'existence de ce premier texte était de "formuler certains principes généraux de comportement loyal dans les relations entre institutions financières, commerçants ou prestataires de services et consommateurs titulaires de cartes"[15]. Déjà, la volonté de favoriser l'application rapide et efficace des nouvelles technologies par la formulation de ces principes était affirmée[16]. Le triple objectif de cette recommandation était d'apporter aux consommateurs sécurité et commodité, aux prestataires de services et émetteurs un gain de productivité et une sécurité, et à l'industrie européenne un marché opérateur[17].

Une lecture rapide de la recommandation permet de noter les principes généraux suivants: affirmation de la nécessité d'un écrit pour les contrats conclus entre émetteur et consommateur (contrats qui doivent faire l'objet d'une demande préalable); la tarification doit être fixée de façon transparente; les conditions du contrat sont librement négociables; les conditions de résiliation doivent être connues du consommateur avant la conclusion du contrat[18]. Le paiement électronique est déclaré irréversible, l'ordre donné au moyen d'une

[12] Considérant 12.

[13] Recommandation 87/598/CEE portant sur un code européen de bonne conduite en matière de paiement électronique, relations entre institutions financières, commerçants-prestataires de services et consommateurs, *J.O.C.E.* L 365, 72 du 24 novembre 1987.

[14] Recommandation 88/590/CEE, *J.O.C.E.* L 317, 55 du 24 novembre 1988.

[15] 10ème considérant introductif.

[16] 11ème considérant introductif.

[17] Pour plus de commentaires sur cette recommandation, le lecteur se reportera à l'article de M. SCHAUSS et X. THUNIS, *Droit de l'informatique et des télécoms*, 1988/1, 52.

[18] Partie III du Code européen de bonne conduite en matière de paiement électronique "Principes Généraux".

carte de paiement étant irrévocable. La recommandation entend ici assurer la sécurité des paiements en interdisant toute opposition ultérieure. En cas de perte ou de vol, le consommateur doit prendre "toutes précautions raisonnables propres à assurer la sécurité de la carte émise et s"en tenir aux conditions particulières [...] du contrat"[19].

2. La recommandation du 17 novembre 1988

5. On retrouve ici des principes énoncés dans la recommandation de 1987 tels que la nécessité d'un contrat écrit et d'une demande préalable, la mention de la base de calcul des frais, mais la recommandation de 1988 va beaucoup plus loin: (1) son *champ d'application* n'est pas limité aux seules opérations de paiement effectuées par carte: elle vise tout paiement électronique effectué avec ou sans carte de paiement (banque à domicile, opérations de retraits et dépôts), ainsi que les paiements non électroniques effectués par carte; (2) elle contient des dispositions importantes relatives à la forme et au contenu[20] des clauses contractuelles qui doivent être établies par écrit, en des termes aisément compréhensibles et dans la langue généralement utilisée là où le contrat est proposé; (3) des obligations sont imposées à l'émetteur et au titulaire dans le souci de prévenir les incidents de paiements: le *titulaire* est soumis à des obligations de *prudence* quant à l'utilisation de son moyen de paiement, et à des obligations de *vigilance*: il doit informer le titulaire de tout incident; les obligations de *l'émetteur* s'inscrivent dans le cadre classique des obligations de sécurité[21], avec en plus l'obligation de mettre ses clients en mesure de lui adresser une notification 24 heures sur 24; (4) enfin et surtout, les dispositions les plus fondamentales de cette recommandation résident dans le souci de *répartition des risques entre les parties concernées*: la limitation de la res-

[19] Partie IV du Code "Dispositions complémentaires".

[20] Les clauses contractuelles doivent préciser si le débit ou le crédit des opérations est instantané et le cas échéant le délai dans lequel les opérations sont débitées ou créditées; et pour les opérations donnant lieu à l'établissement d'une facture, le délai dans lequel la facture est établie.

[21] L'émetteur ne doit pas divulguer les données confidentielles concernant le titulaire, il doit conserver un relevé des pièces justifiant les opérations, il est responsable de la non-exécution ou de l'exécution fautive des opérations et des opérations non autorisées par le titulaire, il lui incombe d'apporter la preuve que les opérations ont été correctement enregistrées et comptabilisées et n'ont pas été affectées par une panne technique ou une déficience du système.

ponsabilité du titulaire[22] après la notification de l'incident de paiement (perte, vol, enregistrement d'opérations non autorisées, erreur ou irrégularité) à l'émetteur; et le *plafonnement de la responsabilité du titulaire* à 150 Écus, sauf s'il a fait preuve de négligence extrême ou a agi frauduleusement (art. 8.3).

B. Contenu de la recommandation de 1997

6. La recommandation du 30 juillet 1997 procède de cette même philosophie d'assurer la sécurité des systèmes de paiement électronique tout en respectant les intérêts des parties concernées. Elle entend "contribuer à l'avènement de la société de l'information, en particulier du commerce électronique, en suscitant une plus grande confiance de la clientèle envers ces instruments et leur plus large acceptation par les commerçants"[23].

1. Champ d'application et définitions

7. La recommandation a un champ d'application très étendu qui vise toutes les opérations effectuées à partir d'un instrument de paiement électronique. Elle consacre également la monnaie électronique, ce qui est nouveau si l'on compare aux recommandations précédentes. Les dispositions du texte sont applicables aux transferts de fonds effectués au moyen d'un instrument de paiement électronique, aux retraits d'argent liquide, à l'accès au compte, aux opérations de chargement et déchargement d'instruments de monnaie électronique. Sont exclus les paiements par chèque et les fonctions de garantie des paiements par chèque assurées par certaines cartes.

Elle définit les notions suivantes: instrument de paiement électronique, instrument de paiement d'accès à distance, instrument de monnaie électronique, institution financière, émetteur et titulaire. Il est intéressant de noter que sous la notion "d'émetteur", les organismes financiers ne sont pas les seuls visés: la qualification est ouverte à toute personne qui, dans le cadre de son activité professionnelle, met un instrument de paiement à la disposition d'un tiers. On

[22] Cette limitation de la responsabilité du titulaire procède d'un véritable renversement de situation, basé sur l'idée que l'émetteur est plus à même que le titulaire de prendre en charge les conséquences financières d'une perte, d'un vol ou de toute erreur ou irrégularité (à condition toutefois que ce dernier n'ait pas fait preuve de négligence extrême ou agit frauduleusement). Voir X. THUNIS, *The second european recommendation concerning payment systems: new obligations for card users?* in *Journal of International Banking Law*, March 1992, vol. 7, issue 3, 101.

[23] Considérant 4 de la recommandation.

pense notamment aux magasins qui proposent des cartes de paiement ou de crédit à leurs clients: ils tombent alors sous le coup de la qualification d'émetteur, et devront se conformer avec les exigences de la recommandation.

Il faut toutefois noter que la recommandation reprend le terme communément utilisé de "monnaie électronique". Les unités chargées sur des cartes rechargeables de type carte Proton développée en Belgique, ou stockées sur une mémoire d'ordinateur, ne sont en effet pas de la monnaie. Les caractéristiques principales de la monnaie sont d'avoir cours légal et d'être immédiatement libératoire: le cours légal interdit au créancier de refuser la monnaie comme moyen de paiement, le caractère immédiatement libératoire implique qu'aucune transition par un système tiers n'est nécessaire. Les supports visés – carte Proton ou mémoire d'ordinateur – ne correspondent clairement pas à ces critères: le titulaire d'une carte Proton ne peut exiger d'un tiers qu'il accepte la carte en paiement, et le passage par un système tiers pour valider le paiement est nécessaire. La recommandation reprend donc à tort le terme générique de "monnaie électronique"; il serait souhaitable d'introduire un nouveau terme, par exemple le terme d'"instrument de paiement rechargeable par voie électronique".

2. Transparence des conditions applicables aux opérations

8. La recommandation prévoit des informations minimales contractuelles et des informations à transmettre postérieurement aux opérations.

2.1 Informations minimales relatives aux conditions d'émission et d'utilisation d'un instrument de paiement électronique

9. L'émetteur doit communiquer au titulaire – par écrit, y compris le cas échéant, par voie électronique – les conditions contractuelles régissant l'émission de l'instrument de paiement en cause, dès la signature du contrat. L'information doit être fournie dans la langue officielle de l'État membre où est proposé l'instrument de paiement électronique[24].

Ces informations portent sur la description de l'instrument de paiement et ses utilisations possibles; une description des obligations et responsabilités respectives du titulaire et de l'émetteur, notamment les précautions élémentaires que doit prendre le titulaire pour assurer la sécurité de l'instrument de paiement; le délai de débit et de crédit du compte ainsi que la date de valeur; les types

[24] Ces exigences étaient déjà présentes dans les recommandations de 1987 et 1988.

de frais à charge du titulaire[25] ainsi que le délai dans lequel ce dernier peut contester une opération et une indication des procédures de réclamation dont il dispose. Une clause supplémentaire prévoit le montant des commissions et le cours de change de référence utilisé dans le cadre d'opérations se réalisant à l'étranger, c'est-à-dire en dehors du pays d'émission ou d'affiliation[26].

2.2 Informations postérieures à l'opération

10. L'émetteur doit fournir au titulaire les informations relatives aux opérations effectuées grâce à l'instrument de paiement: identification des opérations, montant débité, montant des commissions et frais. Les informations doivent être aisément compréhensibles et être présentées sous forme écrite, y compris, le cas échéant, par voie électronique. Ces informations doivent permettre au titulaire d'identifier l'opération, le montant débité et le montant éventuel de commissions et de frais appliqués à certains types d'opérations.

11. Le par. 2 de l'art. 4 précise que dans le cas d'un instrument de monnaie électronique, le titulaire doit avoir la possibilité de connaître les cinq dernières opérations effectuées, ainsi que la valeur résiduelle stockée sur l'instrument. Cette disposition est importante dans le cadre de la responsabilité de l'émetteur exposée à l'art. 8 § 4[27]: l'émetteur est responsable de la perte de toute valeur stockée sur l'instrument et de l'exécution incorrecte des opérations effectuées par le titulaire. Cette disposition permet de connaître la valeur stockée sur l'instrument et donc l'étendue de la responsabilité de l'émetteur qui devra recréditer le compte du titulaire du montant équivalent à la valeur résiduelle.

Pour autant, la recommandation ne prévoit pas d'imposer à l'émetteur de rembourser le titulaire en cas de perte ou de vol de son instrument de monnaie électronique. Seuls les incidents dus à un dysfonctionnement de l'instrument, du dispositif, du terminal ou de tout autre équipement agréé sont visés, pour autant que ce dysfonctionnement n'ait pas été provoqué par le titulaire. L'émetteur n'est en effet pas en mesure – à l'heure actuelle – de bloquer

[25] Les frais comprennent: le montant des frais initiaux et des frais de cotisation annuels, la nature des commissions et tous frais payables par le titulaire à l'émetteur, le taux d'intérêt éventuellement appliqué ainsi que le mode de calcul.

[26] Cette clause perdra sa raison d'être lors de l'avènement de l'Euro, monnaie unique: les transactions réalisées par le réseau sont à 95% des transactions inter européennes. Toutefois, elle gardera sa pertinence pour les transactions qui se réaliseront avec des pays communautaires n'ayant pas souhaité faire partie de l'Union Économique et Monétaire, ainsi que pour les pays qui seront exclus en vertu des critères de convergence.

[27] V. *infra* point 16.

l'utilisation de l'instrument de monnaie électronique suite à un vol ou une perte. Le titulaire en subira donc les pertes[28].

Toutefois, rien n'interdit de penser que la technique mettra un jour les émetteurs en mesure d'empêcher l'utilisation d'un instrument de monnaie électronique en cas de vol ou de perte. Dans ce cas, la responsabilité des émetteurs devra être étendue au remboursement de la valeur résiduelle de l'instrument.

3. Obligations et responsabilités des parties au contrat

12. Les dispositions de la recommandation visent à répartir les obligations et responsabilités entre les parties impliquées dans le système, le titulaire et l'émetteur. L'idée sous-jacente de cette répartition est d'inciter les parties impliquées à prendre les mesures adéquates pour prévenir les incidents.

3.1 Le titulaire

3.1.1 Obligations

13. Le titulaire se voit imposer une obligation d'utilisation de son instrument de paiement en "bon père de famille": il doit faire preuve de diligence pour assurer la sécurité de son instrument de paiement, son premier devoir étant de garantir la confidentialité de son numéro d'identification[29]. Obligation lui est faite de notifier à l'émetteur toute perte, vol, imputation frauduleuse à son compte, erreur ou irrégularité. Cette disposition, déjà présente dans la recommandation de 1988[30], a pour effet de limiter sa responsabilité après la notification de l'incident à l'émetteur (on retrouve là aussi le plafonnement de sa responsabilité à 150 Écus, voir *infra* point **23.**).

[28] Les émetteurs se justifient d'ailleurs en faisant le parallèle entre l'instrument de monnaie électronique et le porte-monnaie "physique": toute perte d'une valeur stockée sur l'instrument équivaut à la perte d'un billet contenu dans son porte-monnaie "physique".

[29] On retrouve d'ailleurs ce principe dans la jurisprudence belge: un arrêt du tribunal de Bruxelles en date du 28 janvier 1987 (in *Journal des Tribunaux* 1987, 601) avait considéré que le propriétaire de la carte avait commis une faute en ne restituant pas sa carte (au moment de la clôture de son compte), en ne la détruisant pas alors qu'il s'y était engagé, en la jetant à la poubelle et en permettant à un tiers de découvrir le code secret alors qu'il s'était engagé contractuellement à conserver soigneusement sa carte, à ne communiquer à personne le numéro de code secret et à avertir la banque de la perte, du vol et de tout risque d'usage abusif. Voir la "Chronique de jurisprudence: l'informatique" (1987-1994) de J.-P. BUYLE, L. LANOYE, Y. POULLET et V. WILLEMS, in *Journal des Tribunaux* 16 mars 1996, n° 38.

[30] V. *supra* point 4.

L'obligation de ne pas révoquer une instruction de paiement est réaffirmée, avec toutefois une exception supplémentaire, qui n'était pas prévue en 1988, et qui vise les instructions relatives à des opérations dont le montant n'est pas connu: dans ce cas, l'irrévocabilité des instructions de paiement ne joue pas.

3.1.2 Responsabilités

14. Jusqu'à la notification, le titulaire est responsable des pertes consécutives à la perte ou au vol de son instrument de paiement, dans la limite d'un plafond déjà fixé en 1988 à 150 Écus. Ce plafond n'est cependant pas applicable dans les cas où le titulaire a agi avec une négligence extrême ou frauduleusement. Sa responsabilité s'arrête dès lors qu'il a rempli son obligation de notification auprès de l'émetteur, avec toujours la même exception liée à l'action frauduleuse du titulaire.

Par dérogation avec les principes ci-dessus énoncés, *la responsabilité du titulaire n'est pas engagée si l'instrument de paiement a été utilisé sans présentation physique ou sans identification électronique.* L'art. 6 § 3 précise que la seule utilisation d'un code confidentiel ou de tout élément d'identification similaire ne suffit pas pour engager la responsabilité du titulaire: celui-ci ne sera donc pas engagé par une simple communication du numéro apparent de sa carte. Cette disposition fondamentale fait échec à l'usage actuel des contrats de mise à disposition de cartes bancaires – contrat que tout titulaire signe avec l'émetteur pour disposer d'une carte bancaire – qui transfèrent la responsabilité des paiements effectués par carte, même si aucun bordereau n'a été signé ou aucun code secret communiqué. Cette disposition fondamentale doit contraindre les émetteurs à adopter des mesures permettant une identification électronique certaine du titulaire, autre que le code confidentiel. Des solutions de cryptage devront éventuellement être envisagées.

3.2 L'émetteur

3.2.1 Obligations

15. L'émetteur dispose de la faculté de modifier les conditions du contrat pourvu qu'il en informe le titulaire dès que possible[31]. Ce dernier dispose alors

[31] Cette disposition ne s'applique pas dans le cadre de modification significative du taux intérêt effectif: la modification prend effet à la date indiquée lors de sa publication (art. 7 1 alinéa 2).

d'un délai d'au moins un mois pour dénoncer le contrat. Une fois le délai écoulé sans dénonciation de sa part, le titulaire est réputé accepter les conditions notifiées.

L'émetteur est soumis à des obligations classiques dans le cadre de la gestion d'un compte et d'un instrument de paiement: il doit s'abstenir de divulguer le numéro d'identification personnel du titulaire et de lui envoyer un instrument de paiement électronique non sollicité – sauf hypothèse de remplacement; il doit conserver un relevé interne des opérations pendant une période suffisamment longue, s'assurer que des moyens appropriés sont à la disposition du titulaire pour effectuer une notification[32]. En cas de différend, il doit apporter la preuve que l'opération a été correctement enregistrée et comptabilisée, et qu'il n'y a pas eu d'incident technique ou autre défaillance.

3.2.2 Responsabilités

16. L'émetteur est responsable de l'inexécution ou de l'exécution incorrecte des opérations transferts de fonds, retraits d'argent liquide et chargement ou déchargement d'un moyen de paiement électronique – y compris les opérations effectuées à partir de dispositifs qui ne sont pas sous son contrôle direct. La seule exception valablement acceptée est relative aux opérations effectuées à partir de dispositifs ou terminaux non agréés par l'émetteur.

Il est également responsable pour les opérations effectuées sans autorisation du titulaire, et de toute erreur ou irrégularité commise dans la gestion de son compte qui lui est imputable. L'étendue de la responsabilité de l'émetteur porte sur le montant de l'opération non exécutée ou incorrectement exécutée – éventuellement augmentée d'intérêts – et sur la somme nécessaire pour rétablir le titulaire dans la situation où il se trouvait avant l'opération non autorisée. La responsabilité des autres conséquences financières liées à l'opération en cause lui incombe également.

Concernant les instruments de monnaie électronique, l'émetteur est responsable de la perte de toute valeur stockée sur cet instrument[33] et de

[32] Dans le cas d'une notification téléphonique, une confirmation écrite devra être envoyée par l'émetteur au titulaire pour prouver que la notification a bien été effectuée. Cette preuve est importante puisque le titulaire est exonéré de sa responsabilité à compter de la notification, mais une question demeure: que se passe-t-il si l'émetteur n'envoie pas de confirmation? La preuve de la notification incombera alors au titulaire.

[33] D'où l'intérêt de la disposition prévue à l'art. 4 § 2 concernant la vérification des cinq dernières opérations effectuées, ainsi que la valeur résiduelle stockée sur l'instrument.

l'exécution incorrecte des opérations effectuées par le titulaire lorsque la perte ou l'inexécution résulte d'un dysfonctionnement d'un équipement agréé, à condition toutefois que ce dysfonctionnement ne soit pas provoqué par le titulaire.

4. Notification, règlement des différends et dispositions finales

17. L'émetteur doit mettre à la disposition du titulaire des moyens lui permettant de notifier, 24 heures sur 24, la perte ou le vol de son instrument de paiement électronique. Il est tenu de faire tout ce qui est en son pouvoir pour empêcher toute nouvelle utilisation de l'instrument de paiement, même si le titulaire a agi avec une négligence extrême ou de manière frauduleuse.

Les États membres sont invités à s'assurer qu'il existe des moyens adéquats et efficaces de règlement des différends entre titulaires et émetteurs.

Enfin, les émetteurs d'instruments de paiement sont invités à se conformer aux dispositions de la recommandation avant le 31 décembre 1998, ce qui représente un délai de 16 mois à compter de la parution de la recommandation au Journal Officiel des Communautés Européennes. Les États membres doivent prendre les mesures nécessaires pour inciter les émetteurs à prendre en compte la recommandation d'ici le 31 décembre 1998.

II. L'articulation de la recommandation et de la directive contrats à distance

18. L'adoption de cette recommandation constitue à la fois une opportunité d'une part pour les systèmes de paiements électroniques et les personnes concernées – titulaires et émetteurs – qui trouvent la porte grande ouverte à une initiative d'autorégulation, et d'autre part pour les contrats à distance qui voient certaines lacunes de la directive comblées (A); et une solution imparfaite pour les consommateurs pour qui la protection apportée par la recommandation, alliée à celle de la directive, n'est malheureusement pas optimale (B).

A. L'impact positif de la recommandation

19. L'impact est positif à un double point de vue: d'abord une démarche volontariste était nettement préférable à une législation contraignante, eu égard à la constante évolution du domaine des paiements électroniques (1); mais également au vu de la directive contrats à distance qui comporte, nous allons le voir, d'importantes lacunes (2).

1. Au vu des techniques de sécurisation des paiements électroniques

20. L'approche proposée par la recommandation est tout particulièrement intéressante: elle impose au titulaire et à l'émetteur un certain nombre d'obligations et les soumet à un certain nombre de responsabilités dans un double but: un premier qui est de prévenir les incidents de paiement et, le cas échéant, d'en limiter les conséquences; et un second qui procède d'une volonté de contraindre les parties concernées de prendre les mesures nécessaires pour se conformer aux principes exposés.

Le choix d'une approche volontariste était déjà clairement exprimé dans la recommandation de 1987: "[...] vouloir définir dès à présent, au niveau communautaire, de manière rigide et détaillée le fonctionnement de systèmes en pleine mutation, risquerait de conduire à l'établissement de règles rapidement périmées constituant même des freins au développement électronique"[34]. Un texte non contraignant est nettement plus approprié vu le besoin de souplesse dicté par l'évolution rapide de la technologie et des intérêts des différentes parties dans le domaine des systèmes de paiement[35], et offre davantage de possibilités d'adaptation qu'une législation contraignante. Au demeurant, c'est surtout l'approche qui est intéressante: les solutions techniques sont laissées à l'appréciation des parties pour parvenir à une sécurisation des paiements électroniques, les enjeux étant fixés dans le texte.

21. Cette solution paraît d'autant plus justifiée que l'expérience montre que les secteurs concernés ont réagi favorablement à la précédente recommandation en adoptant un "code de bonne conduite"[36]. Ce code a été le fruit de discussions avec les organisations représentatives des consommateurs à travers le Comité consultatif des consommateurs et de consultations avec les services de la Commission européenne. On ne peut que saluer cette collaboration, fondamentale pour prendre en compte les intérêts de toutes les parties en cause, mais il n'empêche que le code est critiquable pour plusieurs raisons: 1) les "discussions" avec les organisations de consommateurs peuvent-elles être considérées comme prenant suffisamment en compte leurs intérêts? Rien n'est

[34] 15ème considérant introductif de la recommandation du 8 décembre 1987.
[35] X. FABRE-BULLE, *Le droit communautaire du paiement électronique*, cit., 67.
[36] V. *supra* point 2.

moins sûr; 2) le code n'a pas été considéré par les experts comme une réponse au texte communautaire, de trop nombreuses divergences étant apparues[37]; 3) sa portée se limite aux trois fédérations européennes des établissements de crédit, ce qui exclut les émetteurs n'en faisant pas partie; et surtout 4) le code est un texte non contraignant dont le non-respect ne comporte pas de sanctions.

L'on ne peut que trop insister sur l'adoption d'un code de conduite[38] comme réponse à la recommandation de 1997 par les parties intéressées, et sur le respect de certaines règles fondamentales quant à son élaboration: 1) tout d'abord, l'élaboration d'un code ne peut intervenir que dans le respect des intérêts de toutes les parties en cause et dans le cadre d'une réelle concertation: les professionnels doivent inclure les organisations représentatives des intérêts des consommateurs dans les négociations, il ne doit en aucune façon consacrer les intérêts d'un acteur en particulier; 2) il doit être soumis à une obligation de transparence; 3) il doit permettre un accès aisé des parties concernées; 4) il doit tenir compte des règles de protection des consommateurs au niveau européen; 5) enfin il doit avoir une force contraignante et doit prévoir des sanctions en cas de non respect (ce qui implique des mécanismes de contrôle) de même que des possibilités de recours – judiciaire, administratif ou autre – pour les consommateurs.

2. Au vu de la directive concernant la protection des consommateurs en matière de contrats à distance[39]

2.1. Les lacunes de la directive

22. La directive contrats à distance, et plus spécialement son art. 8 intitulé "paiement par carte", a suscité de nombreuses critiques. Cet article vise à contraindre les États membres à prendre les mesures appropriées pour que le consommateur puisse d'une part demander l'annulation d'un paiement en cas d'utilisation frauduleuse de sa carte de paiement dans le cadre de contrats à distance couverts par la directive, et d'autre part, en cas d'utilisation frauduleuse, qu'il soit recrédité des sommes versées en paiement ou se les voie restituées. Les principales lacunes de ce texte sont relatives à son champ d'application et à la notion d'utilisation frauduleuse.

[37] V. X. FAVRE-BULLE, *op.cit.* note 112.

[38] La directive relative aux contrats à distance encourage d'ailleurs cette solution dans son art. 11 § 4: "les États membres peuvent prévoir que le contrôle du respect des dispositions de la présente directive soit confié à des organismes autonomes".

[39] Pour une analyse de la directive contrats à distance, v. notamment M. VAN HUFFEL, *développements européens en matière de vente à distance et de commerce électronique* et Y. POULLET, *Transactions via Internet et protection des consommateurs*, in *Verkoop op afstand en telematica*, 1997; B. MISSE, *Droit des Technologies avancées*, in *Revue Alain Bensoussan*, 06/1997 n° 4/5, 268.

2.1.1. Champ d'application

23. L'art. 8 ne vise que les paiements par carte. Cela signifie, *a fortiori*, que le consommateur ne bénéficie pas de la protection s'il utilise un autre moyen de paiement. Or, cette considération a son importance à l'heure de l'avènement de la monnaie électronique et des cartes prépayées. C'est précisément dans le cadre du développement du commerce électronique que les "porte-monnaie électroniques" seront amenés à se développer[40]. Cette technique permet, grâce à une carte à puce, de charger une somme d'argent à partir des mêmes terminaux qui proposent le retrait d'argent liquide. À chaque utilisation, la puce décharge le montant de la transaction vers l'appareil de paiement du vendeur[41]. Pour les transactions *on-line*, dès lors qu'un lecteur de cartes à puce est relié à l'ordinateur du client, les paiements à distance via un porte-monnaie électronique peuvent être effectués. La directive se montre rétrograde en ne prenant pas en considération l'ensemble des nouvelles technologies et des moyens de paiement existants.

D'autre part, la protection ne couvre que les contrats à distance visés par la directive ce qui est d'autant plus restrictif que la notion de "contrat à distance" est définie restrictivement par la directive: selon son art. 2, le texte n'est applicable qu'aux seuls contrats qui utilisent exclusivement une ou plusieurs techniques de communication à distance jusqu'à la conclusion du contrat, y compris la conclusion du contrat elle-même. Cette définition exclut ainsi de la protection des dispositions de la directive les contrats se réalisant seulement partiellement à distance, notamment lorsqu'à un moment donné les parties sont amenées à se rencontrer physiquement, même si l'essentiel du contrat s'est réalisé à distance.

[40] Le porte-monnaie électronique présente l'avantage de s'adapter à la fois au commerce électronique, mais également d'être utilisable dans la réalité. Cet alliance du paiement "réel" et "virtuel" le rend plus avantageux que l'E-cash – technique développée par Digicash permettant, grâce à un logiciel *ad hoc*, d'effectuer des paiements sur réseau – qui ne s'adapte pas aux paiements réels. V. sur ce sujet P. HERBIN, *Les nouveaux moyens de paiement sécurisés sur Internet*, in FUNDP, 1997, 38 ss.

[41] Le système est nettement moins onéreux que la classique carte bancaire qui requiert une communication avec le système à chaque transaction: ici, le porte-monnaie électronique n'est déchargé de l'appareil du vendeur qu'une fois par jour et ne nécessite donc qu'une seule communication. V. *ibid.*, 41.

2.1.2 La notion d'utilisation frauduleuse

24. La protection accordée à l'art. 8 ne vise que les hypothèses "d'utilisation frauduleuse", sans toutefois définir cette notion qui *a priori* exclut les cas de mauvaise exécution, d'inexécution ou de négligence qui peuvent être à l'origine d'un incident de paiement. La protection offerte est donc extrêmement minimaliste et ne répond pas aux besoins légitimes de protection des consommateurs dans leur relation avec les vendeurs à distance. Comment en effet justifier que le consommateur n'ait pas le droit de se voir recrédité d'une somme dont le paiement résulte d'une mauvaise exécution? ou qu'il subisse les conséquences d'une inexécution de son ordre de paiement?

2.2. Les enseignements de la recommandation

25. La recommandation comble les lacunes de la directive: premièrement elle prescrit des mesures applicables pour toutes les opérations de paiements, quelque soit le type d'instrument utilisé, et deuxièmement elle a vocation à s'appliquer à tous les contrats, que ces derniers se réalisent à distance ou non, et surtout aux contrats qui ne se réalisent que partiellement à distance. À cet égard, il est intéressant de remarquer que la proposition de directive relative aux contrats à distance entre fournisseurs et consommateurs concernant les services financiers ne comporte aucune disposition similaire à l'art. 8 de la directive contrats à distance: plutôt que de réglementer imparfaitement le domaine des paiements, ce texte a choisi de ne pas essayer de réglementer un domaine qui, de toute évidence, mérite une approche unique.

Bien que la recommandation présente de nombreux avantages et réponde à un certain nombre de faiblesses de la directive vente à distance, la protection qu'elle procure aux consommateurs contractant à distance n'est pas optimale. Les principes posés ne répondent pas en effet à toutes les spécificités de la vente à distance, et ne répondent pas par là même occasion à toutes les exigences de protection des consommateurs contractant à distance.

B. La difficile articulation de la recommandation avec les spécificités de la vente à distance: le cas du droit de rétractation

1. Exposé du problème

26. La directive offre un délai de 7 jours ouvrables au consommateur qui contracte à distance pour se rétracter et revenir sur le contrat. Ce droit de

rétractation exposé à l'art. 6 de la directive[42] a pour but de permettre au consommateur de renoncer librement au contrat, sans mentionner de motif à son revirement. L'absence physique du consommateur lorsqu'il commande un bien ou un service justifie ce délai de rétractation. La directive précise que la renonciation doit s'exercer sans pénalité pour le consommateur: il doit se retrouver dans une situation semblable à celle dans laquelle il se trouvait avant de contracter. Cette disposition implique que, dans l'hypothèse où une partie ou la totalité du montant du contrat a été versé avant la fin du délai de rétractation, le consommateur doit être remboursé. Et c'est précisément là que la recommandation ne répond pas aux exigences consuméristes: on ne trouve aucun moyen de contraindre le professionnel de rembourser le consommateur en cas de renonciation de sa part.

2. L'absence d'effets de la recommandation quant à l'obligation de remboursement

27. Comme déjà exposé, les États membres ont la double obligation, dans le cadre de la directive contrats à distance, d'adopter des mesures appropriées pour permettre au consommateur 1) de demander l'annulation d'un paiement en cas d'utilisation frauduleuse et 2) d'être recrédité des sommes versées en paiement[43]. L'art. 6 § 2 pose un principe similaire en obligeant le fournisseur au "remboursement des sommes versées par le consommateur". Les dispositions de la recommandation couvrent les premières exigences de la directive, de façon beaucoup large on l'a vu, puisque l'utilisation frauduleuse n'est pas le seul incident de paiement envisagé, mais aucune disposition ne correspond à l'obligation de rembourser le consommateur des sommes versées avant la fin du délai de rétractation. Or, nombreuses sont les hypothèses où le commerçant réclame au consommateur le versement d'une somme d'argent

[42] Cette disposition vaut en grande partie pour les produits, bien que la directive soit aussi applicable aux services. Une exception est en effet prévue à l'art. 6 § 3 au sujet des services: ceux-ci ne bénéficient pas du délai de rétractation si leur exécution a commencé, avec l'accord du consommateur, avant la fin du délai de 7 jours ouvrables. La validité de cette exception est d'autant plus compréhensible dans le domaine des services en ligne dont le paiement et l'exécution se font très souvent *on-line*: comment imaginer une rétractation pour un service qui est transmis quasi-immédiatement au consommateur (par exemple par téléchargement ou accès direct à une information) et donc déjà "consommé"?

[43] Le propre d'une directive étant de fixer les objectifs tout en laissant les États membres destinataires libres des moyens à mettre en œuvre et de la forme pour les atteindre: art. 189 du traité de Rome.

en acompte du paiement final qui intervient une fois le bien livré. Cet acompte est donc versé pendant la période des 7 jours donnée au consommateur pour se rétracter. Si le consommateur use de sa faculté de renoncer au contrat, comment lui garantir le remboursement des sommes qu'il a déjà versées?

28. L'absence d'effets de la recommandation quant à l'obligation de remboursement se manifeste à plusieurs égards:

(1) tout d'abord la relation émetteur – titulaire visée par la recommandation n'est pas la même que celle visée dans la directive contrats à distance: dans cette dernière, c'est le vendeur et le consommateur qui sont visés. Si le consommateur et le titulaire peuvent être assimilés, tout vendeur n'est pas un émetteur d'instrument de paiement. On l'a vu, la notion d'émetteur est entendue au sens large dans la recommandation puisqu'elle ne se limite pas aux institutions financières, mais cela ne fait pas de tout vendeur un émetteur d'instrument de paiement. Les obligations et responsabilités décrites dans la recommandation ne s'appliquent donc pas *a fortiori* à tous les vendeurs;

(2) ensuite, la volonté pour le consommateur de se voir rembourser les sommes versées en cas de renonciation de sa part est une situation qui ne correspond pas aux hypothèses énoncées à l'art. 8 § 1 de la recommandation, mettant en jeu la responsabilité de l'émetteur: on ne se situe ni dans le cas d'une inexécution, ni d'une exécution incorrecte, ni d'une perte, ni d'un vol, ni d'une opération effectuée sans le consentement du titulaire, ni d'une erreur, ni d'une irrégularité commise dans la gestion du compte du titulaire. Au contraire, le versement de la somme correspond bien à un acte volontaire du titulaire dont l'authenticité ne peut être mise en doute, et que le celui-ci ne conteste d'ailleurs pas. La recommandation n'apporte donc pas de solutions à la question du remboursement des sommes versées anticipativement par le consommateur.

3. Les autres solutions envisageables

29. La réponse à cette délicate question du remboursement ne se trouvant pas dans la recommandation relative aux instruments de paiement électronique, y a-t-il ailleurs d'autres solutions?

3.1. La politique de remboursement

30. Afin de répondre aux exigences des consommateurs qui, de toute évidence, n'utiliseront pas la technique de la vente à distance si la sécurité de voir les sommes versées avant la fin du délai de rétractation n'est pas garantie, les

professionnels devront résoudre l'épineuse question du remboursement. Une première technique consisterait à afficher une politique claire de remboursement, garantissant au consommateur un remboursement facile et rapide des sommes versées avant l'exécution du contrat en cas de renonciation. Cette politique de remboursement serait valable pour toutes les hypothèses où un versement anticipé a été effectué par le consommateur, que le remboursement soit justifié par une rétractation de sa part, l'impossibilité de livraison par le vendeur, ou encore l'absence d'exécution du contrat par le vendeur. Le remboursement porte sur la totalité des sommes versées anticipativement par le consommateur[44]. Le remboursement s'effectuerait alors dès la renonciation du consommateur, ou autre hypothèse d'impossibilité de livraison ou de non-exécution par le vendeur[45].

31. Une autre technique pourrait éventuellement venir s'ajouter à la politique de remboursement: la technique du blocage de la somme versée anticipativement par le consommateur. La somme versée serait bloquée sur un compte par un organisme tiers jusqu'à l'expiration du délai de rétractation, et ne serait versée sur le compte du vendeur qu'en l'absence de renonciation du consommateur et qu'à condition que le bien ait été livré par le vendeur. En cas contraire, l'organisme tiers serait informé que le montant versé doit retourner au consommateur. Cette solution présente l'avantage de ne pas conditionner le remboursement à la seule volonté du vendeur, mais ne s'avère malgré tout pas optimale: la somme immobilisée profiterait à l'organisme tiers et pourrait mener à des abus tels que la restitution tardive.

3.2. Le cautionnement ou la "labellisation" des sites

32. Le remboursement pourrait encore être garanti par la technique de la "labellisation" du site du vendeur. Un label assurant un gage de qualité et s'affichant sur le site permettrait au consommateur de vérifier le sérieux du vendeur. Un organisme tiers[46] accorderait son label aux vendeurs qui devraient préalablement s'engager à respecter certaines règles, notamment en matière de politique de remboursement. L'insertion du label sur le site pourrait mettre

---

[44] Comme le précise l'art. 6 de la directive, la rétractation doit se réaliser sans frais pour le consommateur.

[45] À noter que la directive prévoit un délai pour que le remboursement s'effectue: "il doit intervenir dans les meilleurs délais et en tout cas dans les 30 jours" (art. 6 § 2).

[46] Les sociétés d'audit se montrent d'ailleurs très intéressées par cette formule: elles voient là un nouveau marché, à l'image de TRUSTe aux États-Unis.

les consommateurs à même de vérifier par eux-mêmes les garanties offertes, par le biais d'un lien entre le site du vendeur et celui de l'organisme de labellisation. Bien sûr, cette technique, qui s'est déjà développée aux États-Unis dans le domaine de la protection de la vie privée[47], nécessite une détermination claire des enjeux et responsabilités en cause: il faut s'interroger sur la responsabilité de l'organisme qui délivre le label, de même, que se passe-t-il en cas d'utilisation abusive du label? ou en cas de non-respect des règles affichées? Autant de questions, et il y en a d'autres, qui devront nécessairement être résolues avant de développer cette technique.

Une initiative similaire existe aux États-Unis en matière de commerce électronique: le *CPA WebTrust*, créé par l'*AICPA* (*American Institute of Certified Public Accountants*), qui est considéré comme un label unique d'assurance pour le commerce électronique[48]. L'idée est de partir de la législation relative aux pratiques du commerce et de vérifier qu'elle est correctement mise en œuvre par les sites *Web*. Trois principes servent de guide: 1) l'information sur les pratiques du commerce: le site *WebTrust* met à la disposition des autres sites la législation existante en matière de pratiques commerciales applicables aux transactions réalisées par voie électronique, 2) l'intégrité des transactions: le site assure un contrôle effectif pour s'assurer que les ordres des clients sont correctement exécutés, et 3) la protection de l'information: le site s'assure que les informations personnelles sont protégées et ne font pas l'objet d'une exploitation commerciale. Concrètement, *WebTrust* examine la conformité des sites avec les prescriptions en matière commerciale, et en cas de succès effectue un rapport établissant la conformité du site. Le label *WebTrust* est alors accordé au site et s'affiche sur le site, offrant ainsi un accès direct des consommateurs par le biais d'un *link*. *WebTrust* effectue une révision de chaque site tous les 4 mois qui détermine le maintien ou non du label en fonction du respect de la législation, avec une fréquence plus soutenue pour les sites particulièrement dynamiques. Selon *WebTrust*, cette expérience a montré que l'existence de ce site a entraîné une augmentation de la confiance des utilisateurs.

[47] *TRUSTe, the privacy challenge: "TRUSTe is dedicated to building your trust in providing information and making purchases online [...], to promoting trust and protecting privacy on the Internet". Available on the Internet at the following address:* http://truste.org

[48] Pour plus d'informations, le lecteur se reportera au site www.aicpa.org/webtrust

Conclusion

33. Comment ne pas applaudir l'initiative de la Commission européenne qui a choisi délibérément de se reposer sur les organismes concernés pour qu'ils adoptent eux-mêmes leur réglementation, propice à une démarche volontaire tellement plus proche des préoccupations des secteurs concernés: ces solutions sont en effet prises au niveau le plus approprié et leur souplesse permet leur évolution[49]. On rappellera toutefois la nécessité d'inclure tous les acteurs dans le processus d'élaboration afin que l'autorégulation ne consacre pas l'intérêt d'une seule partie, ainsi que la nécessaire force contraignante qui doit être accordée aux codes de conduite sans quoi leur utilité ne serait qu'illusoire. L'adoption du "code de bonne conduite" en 1990 comme réponse à la recommandation de 1988 est à cet égard un exemple positif qui doit susciter une réaction similaire des secteurs concernés et qui permettrait, ne l'oublions pas, d'éviter l'adoption d'un texte contraignant par la Commission européenne.

En matière de vente à distance et de politique de remboursement, que ce soit afficher une politique de remboursement, bloquer les sommes versées par le consommateur jusqu'à la fin du délai de rétractation ou encore faire appel à un label garantissant le site, ce sont autant de solutions différentes dont le but commun est d'accroître la confiance des utilisateurs/consommateurs dans le commerce électronique.

Ces suggestions doivent constituer des pistes de réflexion à approfondir. Sans doute les professionnels adapteront-ils ces solutions à leurs particularités, ou même en définiront-ils d'autres, mais ils devront, en tout état de cause, offrir des garanties sérieuses au consommateur afin qu'il ne se sente pas exposé à plus de risques dans le cadre du commerce électronique que dans le cadre du commerce traditionnel.

[49] Y. POULLET, *op.cit.*, 161.